

Commutative Algebra

Computational Methods

13-04

- [1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze. Computation of the decomposition group of a triangular ideal. *Appl. Algebra Engrg. Comm. Comput.*, 15(3-4):279–294, 2004.
- [2] Fatima Abu Salem, Shuhong Gao, and Alan G. B. Lauder. Factoring polynomials via polytopes. In *ISSAC 2004*, pages 4–11. ACM, New York, 2004.
- [3] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. Comparison between XL and Gröbner basis algorithms. In *Advances in Cryptology—Asiacrypt 2004*, volume 3329 of *Lecture Notes in Comput. Sci.*, pages 338–353. Springer, Berlin, 2004.
- [4] Philippe Aubry and Marc Moreno Maza. Triangular sets for solving polynomial systems: A comparative implementation of four methods. *J. Symbolic Comput.*, 28(1-2):125–154, 1999.
- [5] Mohamed Ayad and Peter Fleischmann. On the decomposition of rational functions. *J. Symbolic Comput.*, 43(4):259–274, 2008.
- [6] Aurélie Bauer and Antoine Joux. Toward a rigorous variation of Coppersmith’s algorithm on three variables. In *Advances in cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 361–378. Springer, Berlin, 2007.
- [7] Karim. Belabas, Mark van Hoeij, J. Klüners, and Allan Steel. Factoring polynomials over global fields. *Journal de Théorie des Nombres de Bordeaux*, (21):15–39, 2009.
- [8] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt. Computing restrictions of ideals in finitely generated k -algebras by means of Buchberger’s algorithm. *J. Symbolic Comput.*, 41(3-4):372–380, 2006.

- [9] Alin Bostan, Bruno Salvy, and Éric Schost. Fast algorithms for zero-dimensional polynomial systems using duality. *Appl. Algebra Engrg. Comm. Comput.*, 14(4):239–272, 2003.
- [10] Richard Brent and Paul Zimmermann. A multi-level blocking distinct degree factorization algorithm. In *Finite Fields and Applications*, volume 461 of *Contemporary Mathematics*, 47–58 pages. 2008.
- [11] Michael Brickenstein and Alexander Dreyer. PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials. *J. Symbolic Comp.*, 44(9):1326–1345, 2009.
- [12] Michael Brickenstein, Alexander Dreyer, Gert-Martin Greuel, Markus Wedler, and Oliver Wienand. New developments in the theory of Gröbner bases and applications to formal verification. *J. Pure Appl. Algebra*, 213(8):1612–1635, 2009.
- [13] Stanislav Bulygin and Ruud Pellikaan. Bounded distance decoding of linear error-correcting codes with Gröbner bases. *J. Symb. Comput.*, 44(12):1626–1643, 2009.
- [14] Mihai Cipu. Gröbner bases and Diophantine analysis. *J. Symbolic Comput.*, 43(10):681–687, 2008.
- [15] Jennifer de Kleine, Michael Monagan, and Allan Wittkopf. Algorithms for the non-monic case of the sparse modular GCD algorithm. In *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation: ISSAC’05*, pages 124–131 (electronic). ACM, New York, 2005.
- [16] Wolfram Decker and Theo de Jong. Gröbner bases and invariant theory. In *Gröbner bases and applications (Linz, 1998)*, volume 251 of *London Math. Soc. Lecture Note Ser.*, pages 61–89. Cambridge Univ. Press, Cambridge, 1998.
- [17] Harm Derksen. Computation of invariants for reductive groups. *Adv. Math.*, 141(2):366–384, 1999.
- [18] Harm Derksen and Gregor Kemper. *Computational Invariant Theory. Invariant Theory and Algebraic Transformation Groups, I*. Springer-Verlag, Berlin, 2002.

- [19] Clémence Durvye and Grégoire Lecerf. A concise proof of the Kronecker polynomial system solver from scratch. *Expo. Math.*, 26(2):101–139, 2008.
- [20] Tobias Eibach, Enrico Pilz, and Gunnar Völkel. Attacking Bivium using SAT solvers. In *Theory and Applications of Satisfiability Testing, SAT 2008*, volume 4996 of *Lecture Notes in Computer Science*, pages 63–76. Springer, Berlin, 2008.
- [21] Nicholas Eriksson. Toric ideals of homogeneous phylogenetic models. In *ISSAC 2004*, pages 149–154. ACM, New York, 2004.
- [22] Jeffrey B. Farr and Shuhong Gao. Computing Gröbner bases for vanishing ideals of finite sets of points. In *Applied Algebra, Algebraic Algorithms and Error-correcting Codes*, volume 3857 of *Lecture Notes in Comput. Sci.*, pages 118–127. Springer, Berlin, 2006.
- [23] Jeffrey B. Farr and Shuhong Gao. Gröbner bases and generalized Padé approximation. *Math. Comp.*, 75(253):461–473 (electronic), 2006.
- [24] Jean-Charles Faugère, Guillaume Moroz, Fabrice Rouillier, and Mohab Safey El Din. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In *ISSAC '08: International Symposium on Symbolic and Algebraic Computation*, pages 79–86, New York, NY, USA, 2008. ACM.
- [25] Akpodigha Filatei. *Implementation of Fast Polynomial Arithmetic in Aldor*. Master of Science thesis, University of Western Ontario, 2006.
- [26] Shuhong Gao, Daqing Wan, and Mingsheng Wang. Primary decomposition of zero-dimensional ideals over finite fields. *Math. Comp.*, 78(265):509–521, 2009.
- [27] Karin Gatermann. *Computer algebra methods for equivariant dynamical systems*, volume 1728 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2000.
- [28] Karin Gatermann and Frédéric Guyard. Gröbner bases, invariant theory and equivariant dynamics. *J. Symbolic Comput.*, 28(1-2):275–302, 1999.

- [29] V. P. Gerdt and Yu. A. Blinkov. Strategies for selecting non-multiplicative prolongations in computing Janet bases. *Programirovanie*, (3):34–43, 2007.
- [30] Vladimir P. Gerdt. Involutive algorithms for computing Gröbner bases. In *Computational Commutative and Non-commutative Algebraic Geometry*, volume 196 of *NATO Sci. Ser. III Comput. Syst. Sci.*, pages 199–225. IOS, Amsterdam, 2005.
- [31] Vladimir P. Gerdt and Yuri A. Blinkov. On computing Janet bases for degree compatible orderings. In *Proceedings of the 10th Rhine Workshop on Computer Algebra (Basel), 2006*, pages 107–117. University of Basel, Basel, 2006.
- [32] Massimo Giuliatti. Involuppi di k -archi in piani proiettivi sopra campi finiti e basi di Gröbner. *Rendiconti del Circolo Matematico di Palermo*, 48(1):191–200, 1999.
- [33] Marc Giusti, Grégoire Lecerf, and Bruno Salvy. A Gröbner free alternative for polynomial system solving. *J. Complexity*, 17(1):154–211, 2001.
- [34] Marc Giusti and Éric Schost. Solving some overdetermined polynomial systems. In *ISSAC '99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 1–8 (electronic), New York, 1999. ACM.
- [35] Hoans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, and Christiaan van de Woestijne. The Casas-Alvero conjecture for infinitely many degrees. *J. Algebra*, 316(1):224–230, 2007.
- [36] Renault Guénaél and Yokoyama Kazuhiro. Multi-modular algorithm for computing the splitting field of a polynomial. In *ISSAC '08: International Symposium on Symbolic and Algebraic Computation*, pages 247–254, New York, NY, USA, 2008. ACM.
- [37] David Harvey. A cache-friendly truncated FFT. *Theor. Comput. Sci.*, 410(27-29):2649–2658, 2009.
- [38] David Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. *J. Symbolic Comp.*, 44(10):1502–1510, 2009.

- [39] Mikael Johansson. Computation of Poincaré-Betti series for monomial rings. *Rend. Istit. Mat. Univ. Trieste*, 37(1-2):85–94 (2006), 2005.
- [40] Gregor Kemper. Computational invariant theory. In *The Curves Seminar at Queen's. Vol. XII (Kingston, ON, 1998)*, volume 114 of *Queen's Papers in Pure and Appl. Math.*, pages 5–26. Queen's Univ., Kingston, ON, 1998.
- [41] Gregor Kemper. An algorithm to calculate optimal homogeneous systems of parameters. *J. Symbolic Comput.*, 27(2):171–184, 1999.
- [42] Gregor Kemper. The calculation of radical ideals in positive characteristic. *J. Symbolic Comput.*, 34(3):229–238, 2002.
- [43] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):159–176, 2003.
- [44] Simon King. Fast computation of secondary invariants. [arXiv:math/0701270](https://arxiv.org/abs/math/0701270), 13 pages, 2007.
- [45] Simon King. Minimal generating sets of non-modular invariant rings of finite groups. [arXiv:math/0703035](https://arxiv.org/abs/math/0703035), 14 pages, 2007.
- [46] Alexey Koloydenko. Symmetric measures via moments. *Bernoulli*, 14(2):362–390, 2008.
- [47] Teresa Krick. Straight-line programs in polynomial equation solving. In *Foundations of Computational Mathematics: Minneapolis, 2002*, volume 312 of *London Math. Soc. Lecture Note Ser.*, pages 96–136. Cambridge Univ. Press, Cambridge, 2004.
- [48] G. Lecerf. Quadratic Newton iteration for systems with multiplicity. *Found. Comput. Math.*, 2(3):247–293, 2002.
- [49] Grégoire Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *J. Complexity*, 19(4):564–596, 2003.
- [50] Grégoire Lecerf. Fast separable factorization and applications. *Appl. Algebra Engrg. Comm. Comput.*, 19(2):135–160, 2008.

- [51] Xin Li, Marc Moreno Maza, Raqeeb Rasheed, and Eric Schost. High-performance symbolic computation in a hybrid compiled-interpreted programming environment. In *International Conference on Computational Sciences and Its Applications. ICCSA. June 30- July 3, 2008*, pages 331–341. 2008.
- [52] Xin Li, Marc Moreno Maza, and Éric Schost. Fast arithmetic for triangular sets: from theory to practice. In *ISSAC 2007*, pages 269–276. ACM, New York, 2007.
- [53] Xin Li, Marc Moreno Maza, and Éric Schost. Fast arithmetic for triangular sets: from theory to practice. *J. Symbolic Comput.*, 44(7):891–907, 2009.
- [54] A. Marschner and J. Müller. On a certain algebra of higher modular forms. *Algebra Colloq.*, 16:371–380, 2009.
- [55] Mbakop Guy Merlin. *Eziente Losung reeller Polynomialer Gleichungssysteme*. PhD Thesis, Humboldt-Universität, Berlin, 1999.
- [56] V. A. Mityunin and E. V. Pankratiev. Parallel algorithms for Gröbner-basis construction. *J. Math. Sci. (N. Y.)*, 142(4):2248–2266, 2007.
- [57] Michael Monagan and Mark van Hoeij. A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions. <http://www.cecm.sfu.ca/CAG/papers/HoeijMonGCD.pdf>, 36 pages.
- [58] Teo Mora. The FGLM problem and Möller’s algorithm on zero-dimensional ideals. In *Sala, Massimiliano (ed.) and Mora, Teo (ed.) and Perret, Ludovic (ed.) and Sakata, Shojiro (ed.) and Traverso, Carlo (ed.), Gröbner Bases, Coding, and Cryptography*. Springer, Berlin, 2009.
- [59] Marc Moreno Maza, Greg Reid, Robin Scott, and Wenyuan Wu. On approximate triangular decompositions in dimension zero. *J. Symbolic Comput.*, 42(7):693–716, 2007.
- [60] Bernard Mourrain. Generalized normal forms and polynomial system solving. In *ISSAC’05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, pages 253–260 (electronic). ACM, New York, 2005.

- [61] Bernard Mourrain and Philippe Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229 – 240, 2008.
- [62] Jörn Müller-Quade and Rainer Steinwandt. Basic algorithms for rational function fields. *J. Symbolic Comput.*, 27(2):143–170, 1999.
- [63] Jörn Müller-Quade and Rainer Steinwandt. Gröbner bases applied to finitely generated field extensions. *J. Symbolic Comput.*, 30(4):469–490, 2000.
- [64] G. H. Norton and A. Sălăgean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields Appl.*, 9(2):237–249, 2003.
- [65] Graham H. Norton and Ana Sălăgean. Strong Gröbner bases for polynomials over a principal ideal ring. *Bull. Austral. Math. Soc.*, 64(3):505–528, 2001.
- [66] Daniel Robertz. Noether normalization guided by monomial cone decompositions. *J. Symbolic Comp.*, 44(10):1359–1373, 2009.
- [67] Fabrice Rouillier, Mohab Safey El Din, and Éric Schost. Solving the Birkhoff interpolation problem via the critical point method: An experimental study. In Jürgen Richter-Gebert and Dongming Wang, editors, *ADG '00: Revised Papers from the Third International Workshop on Automated Deduction in Geometry (Zurich, 2000)*, volume 2061 of *Lecture Notes in Computer Science*, pages viii+325. Springer-Verlag, Berlin, 2001.
- [68] Luciano Sbaiz, Patrick Vandewalle, and Martin Vetterli. Groebner basis methods for multichannel sampling with unknown offsets. *Appl. Comput. Harmon. Anal.*, 25(3):277 – 294, 2008.
- [69] Roberto La Scala and Viktor Levandovskyy. Letterplace ideals and non-commutative Gröbner bases. *J. Symbolic Comp.*, 44(10):1374–1393, 2009.
- [70] Éric Schost. Degree bounds and lifting techniques for triangular sets. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 238–245 (electronic), New York, 2002. ACM.

- [71] Éric Schost. Complexity results for triangular sets. *J. Symbolic Comput.*, 36(3-4):555–594, 2003.
- [72] Éric Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003.
- [73] R. James Shank and David L. Wehlau. Computing modular invariants of p -groups. *J. Symbolic Comput.*, 34(5):307–327, 2002.
- [74] Jessica Sidman and Seth Sullivant. Prolongations and computational algebra. *Can. J. Math*, 61(4):930–949, 2009.
- [75] Allan Steel. Conquering inseparability: Primary decomposition and multivariate factorization over algebraic function fields of positive characteristic. *J. Symbolic Comput.*, 40(3):1053–1075, 2005.
- [76] Till Stegers. *Faugère’s F5 Algorithm Revisited*. Phd thesis, Technische Universiteit Eindhoven, 2006.
- [77] Rainer Steinwandt. Decomposing systems of polynomial equations. In *Computer Algebra in Scientific Computing—CASC’99 (Munich)*, pages 387–407. Springer, Berlin, 1999.
- [78] Rainer Steinwandt. Implicitizing without tag variables. In *Proceedings of the 8th Rhine Workshop on Computer Algebra*, pages 217–224. 2002.
- [79] Rainer Steinwandt and Jörn Müller-Quade. Freeness, linear disjointness, and implicitization—a classical approach. *Beiträge Algebra Geom.*, 41(1):57–66, 2000.
- [80] Mark van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2):167–189, 2002.
- [81] Pawel Wocjan. *Brill-Noether Algorithm Construction of Geometric Goppa Codes and Absolute Factorization of Polynomials*. PhD thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 1999.